A Novel Encryption Using Nibble Swapping

Dr. S.Kiran[1], Dr. B.Reddaiah[2], D.Naga Sravanthi[3], J.Venkata Sivajaya Sree[4]
Assistant Professor[1],Assistant Professor[2], Student B. Tech (CSE)[3], Student B. Tech (CSE)[4]

***Abstract*-Security is becoming more concern in this eternally changing world of global data communications. Many companies store highly confidential business information and individual information on computers. Security for this information is done by using several mechanisms. Cryptography is the deliberate method which provides security for the data from unauthorized person. This paper proposes multistage encryption algorithm. This paper generates two keys. One from raster scan method and the other from store and forward. In the first stage, caeser cipher substitution method is used, which is computed by using the key, generated from raster scan method. In the second stage perform XOR operation between intermediate cipher and key generated form store and forward method. In the third stage, column wise retrieval and nibble grouping is applied. Because of these techniques, this algorithm is efficient than the existing one.**

Index terms: Raster scan method, Store and forward method, Nibble grouping.

I. INTRODUCTION

Cryptography is the study of furtive writing. It is the art of transferring a decipherable message into one which is indecipherable, and then retransforming that message back into its original form. The message which is in decipherable format is plaintext. The plaintext is converted into cipher text which is in indecipherable form, by applying encryption algorithm. The process of converting cipher text into plaintext is known as decryption. The process of cryptography results in concealing the context of message from all except the sender and the recipient.

Cryptography has many viable applications. Cryptography is used to provide solutions to many problems like confidentiality, data integrity, authentication, non repudiation and access control. Several techniques are used for encryption and decryption. Substitution and transposition are two techniques. In substitution method, each alphabet in text is replaced by other letter systematically, where as in transposition method position of the letters are transferred[1]. There are two basic kinds of encryption algorithms. One is symmetric algorithm and the other is asymmetric algorithm. In symmetric algorithm same keys will be used for both encryption and decryption algorithms. In asymmetric algorithm different keys will be used for encryption and decryption. In an asymmetric system, each user has a public /private key pair where as in symmetric user has only one key. The proposed algorithm follows symmetric cryptographic [3] system.

II.HISTORY

Cryptography is one of the oldest fields of scientific study starts at 4000 years back. The word cryptography comes from the Greek word 'kryptos' and 'graphein'. The most primitive form of cryptography was the simple writing of a message which is not explicable by most people. Cryptography began in egypt, where hieroglyphics were used to adorn the tombs of late rulers and kings.

The early substitution cipher was Caesar cipher by Julius Caesar. Julius Caesar shifts each alphabet in plain text to three positions to communicate with his generals. In Caesar cipher substitution method each alphabet is shifted by fixed number of positions. This is example of mono alphabetic cipher. But it is easy to break. There are no major changes or advancements until the middle ages. Leon Battista Alberti who is the father of western cryptology developed poly alphabetic substitution. This substitution technique allows different cipher alphabets to represent same plaintext alphabet[4].

In the start of 19th century, a new electro mechanical device was deliberated by Herban and it is named as Herban rotar machine. That device consists of single rotar, in which surreptitious key is surrounded in rotating disk. At the end of world war-I, A Germany engineer, Arthur Scherbius, invented an Engima machine which consists of 2 or 3 or even 4 motors. These rotars were rotated with different rates and generate fitting output cipher for given input alphabet.

Up to second world war, the cryptography was mainly used to hide message in military. After that some of the companies were used cryptography to hide their information from other competitors. In 1970, one "crypto group" was developed by IBM. That group was named as Horst -Fiestel. Lucifer is the cipher which was developed by them. Lucifer was called as data encryption standard (DES). In 1997, Nation Bureau standards request for block cipher and accepted DES for that. In that year and in the following years, by using some meticulous search attack, DES was broken. Small size of the encryption key is the main problem with DES. In 2000, Nation Bureau standards accept Rijndael algorithm as block cipher. Now that algorithm is treated as advanced encryption standard.

III. EXISTING WORK

The SDES key generation is done by using permutation method[5]. Two keys are generated from the

SDES key generation algorithm .Among them, select the smallest one as the key. Encryption algorithm is done in three steps by using caesar cipher substitution, transposition and arithmetic and logical operations.

IV. PROPOSED WORK

The proposed work generates a 64 bit random sequence for key generation. Key generation consists of two parts . One is raster scan method and the other is store and forward method. The proposed work constitutes various stages of encryption and decryption algorithm. So that, more security provided for the data from unauthorized access.

A. Raster scan key generation

In raster scan method, the random number sequence bits are divided into group of chunks, and then compute the decimal value for each chunk. Retrieve the corresponding binary bit for each decimal value from random sequence.

Algorithm steps:

Step 1:Initially generate random 64 bit sequence from right to left.

Step 2:Divide those 64 bits into 8 chunks, each chunk consist of 8 bits.

Step 3: Work out decimal number for each chunk.

Step 4:Retrieve the binary bit from random 64 bit sequence From the position of decimal number. **(If the Decimal number is greater than 64, subtracts the decimal number with 64 and then continue.)**

Step 5: Compute the decimal number to the above 8 bit sequence that is referred as key.

Example for raster scan method

Step 1:Random 64 bit sequence is
0000001100001100000110000001000000010000000100100001100100001101

Step 2: Divide this sequence into 8 chunks
00000011|00001100|00011000|00010000|00100000|00100100|00110010|00001101

Step 3: Calculate decimal number for each chunk.
3 12 24 16 32 36 50 13

Step 4: Retrieve the decimal number position bit.
1 0 0 0 0 0 0 1

Step 5: The decimal value for the key is 129.

B. Store and Forward Key generation

In store and forward method, random sequence numbers are divided into group of chunks, and workout decimal for each chunk. At first take the binary bit in the position of decimal value from right to left. Next, take the decimal number position's binary bit starts from the last bit position retrieved.

Algorithm steps

Step 1**:** Consider above random 64 binary bit sequence from right to left.

Step 2: Divide those 64 bits into 8 chunks, each chunk consist of 8 bits.

Step 3: Compute decimal number for each chunk.

Step 4: Retrieve the binary bit from the 64 bit random Sequence corresponding to the first decimal number position.

Step 5: Stores the position of the previously retrieved bit, Next binary bit retrieved process begins from the current stored binary bit position.

Step 6: Compute the decimal number to the above 8 bit sequence that is referred to be as key.

Example for store and forward key generation

Step 1: Random 64 bit sequence is
0000001100001100000110000001000000010000000100100001100100001101

Step 2:Divide this sequence into 8 chunks:
00000011|00001100|00011000|00010000|00100000|00100100|00110010|00001101

Step 3: Calculate decimal number for each chunk.
3 12 24 16 32 36 50 13

Step 4: Retrieve the decimal number position bit.
1 0 0 0 0 0 1 1

Step 5: The decimal value for the key is 131.

C Encryption Algorithm

Round 1:

- For the given plaintext, retrieve the corresponding value from the lookup table.
- Apply Caesar cipher substitution method by using the key generated from raster scan method, for the previous values.
- An intermediate cipher1 is produced by retrieving the corresponding character, for the result of Caesar cipher substitution method, from the look up table.

Round 2:

- Calculate the decimal and binary numbers for intermediate cipher1.
- Perform XOR operation between binary numbers and key generated from the store and forward method.

Round 3:

- Generate 8 random numbers from 0-7.
- Interchanging the column into row wise based on 8 random numbers.
- Compute the decimal number for each row.
- Calculate the hexadecimal value for each decimal number.
- Final cipher is obtained by using nibble swapping.

Flow chart for proposed encryption algorithm

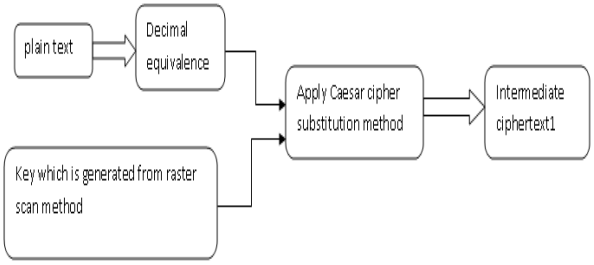

Figure 1: Round 1

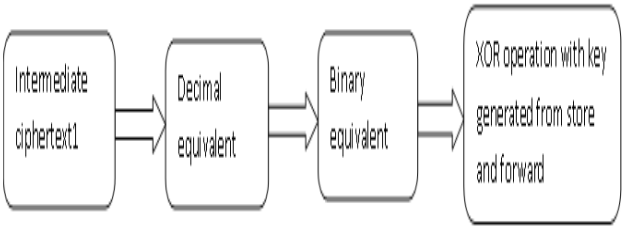

Figure 2: Round 2

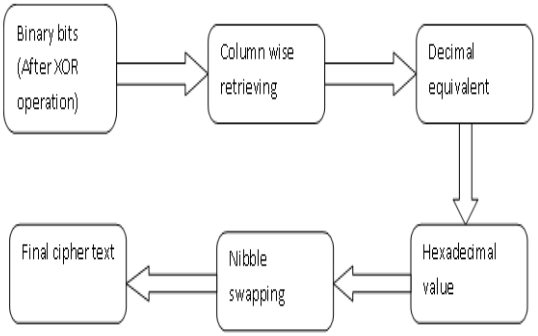

Figure 3: Round 3

D. Decryption Algorithm

Round1: The received ciphertext is shifted based on reverse of nibble grouping. For this result, work out the hexadecimal and the decimal equivalent and then perform row wise retrieving operation.

Round 2: Perform XOR operation between binary bits (obtained after row wise retrieving) and key (generated from store and forward). After that calculate the decimal and equivalent character from the look up table.

Round 3: Apply Caesar cipher substitution method for the decimal equivalent of the above intermediate cipher text1. Work out the equivalent character for the previous values from the look up table, which generates original plaintext.

Flow chart for proposed decryption algorithm

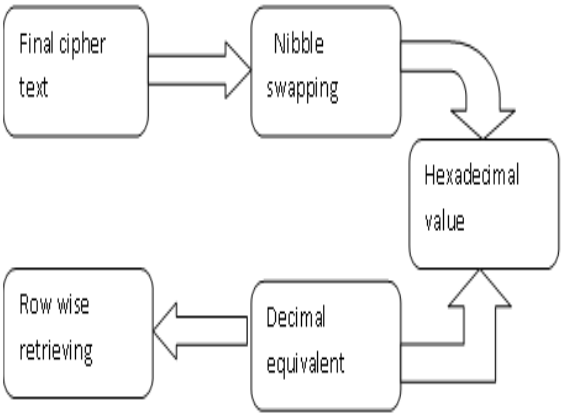

Figure 4: Round1

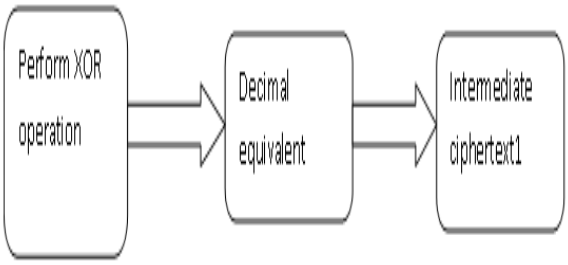

Figure 5: Round 2

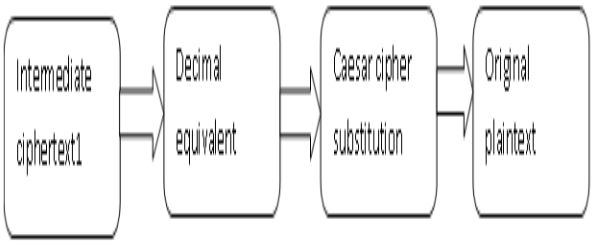

Figure 6: Round 3

Table 1: Arithmetic and logic lookup table

Character	Value	Character	Value
!	0	R	49
“	1	S	50
#	2	T	51
$	3	U	52
%	4	V	53
&	5	W	54
‘	6	X	55
(	7	Y	56
)	8	Z	57
*	9	[	58
+	10	\	59
‘	11	]	60
-	12	^	61
.	13	_	62
/	14	`	63
0	15	a	64
1	16	b	65
2	17	c	66
3	18	d	67
4	19	e	68
5	20	f	69
6	21	g	70
7	22	h	71
8	23	i	72
9	24	j	73
:	25	k	74
;	26	l	75
<	27	m	76
=	28	n	77
>	29	o	78
?	30	p	79
@	31	q	80
A	32	r	81
B	33	s	82
C	34	t	83
D	35	u	84
E	36	v	85
F	37	w	86
G	38	x	87
H	39	y	88
I	40	z	89
J	41	{	90
K	42	|	91
L	43	}	92
M	44	~	93
N	45		
O	46		
P	47		
Q	48		

E. Example for Encryption algorithm

Round 1:

Given plaintext is **security**

Key generated by raster scan is 129

Table 2: substitution and transposition

Plaintext (p)	Corresponding value(v)	C=(v+key) %94	Corresponding character of C
s	82	23	8
e	68	9	*
c	66	7	(
u	84	25	:
r	81	22	7
i	72	13	.
t	83	24	9
y	88	29	>

Intermediate cipher1 is **8*(:7.9>**

Round 2:

Intermediate cipher 1	Decimal equivalent	Binary equivalent	XOR operation
8	23	00010111	10010100
*	9	00001001	10001010
(	7	00000111	10000100
:	25	00011001	10011010
7	22	00010110	10010101
.	13	00001101	10001110
9	24	00011000	10011011
>	29	00011101	10011110

Table 3: arithmetic and logical operations

Round 3:

Order for column wise retrieving is 7 6 3 1 0 4 5 2

Table 4: arithmetic and logical operations

XOR operation	Column wise retrieving	Decimal equivalent	Hexadecimal equivalent
10010100	01010111	87	57
10001010	10011011	155	9B
10000100	00001010	10	0A
10011010	00000000	0	00
10010101	10101101	173	AD
10001110	01010111	87	57
10011011	00000000	0	00
10011110	11111111	255	FF

Table5: Nibble swapping

Hexadecimal equivalent	Final cipher with nibble swapping
57	59
9B	00
0A	A5
00	0F
AD	7B
57	A0
00	D7
FF	0F

Final cipher text is: **5900A50F7BA0D70F**

F. Example for decryption algorithm

Round 1: Table 6: inverse nibble swapping

Final cipher	Nibble swapping
59	57
00	9B
A5	0A
0F	00
7B	AD
A0	57
D7	00
0F	FF

Round 2:

Table 7: arithmetic and logical operations

Nibble swapping in Hexadecimal	Decimal equivalent	Equivalent binary	Row wise retrieving
57	87	01010111	10010100
9B	155	10011011	10001010
0A	10	00001010	10000100
00	0	00000000	10011010
AD	173	10101101	10010101
57	87	01010111	10001110
00	0	00000000	10011011
FF	255	11111111	10011110

Table 8: arithmetic and logical operations

Row wise retrieving	XOR operation	Decimal equivalent	Intermediate ciphertext 1
10010100	00010111	23	8
10001010	00001001	9	*
10000100	00000111	7	(
10011010	00011001	25	:
10010101	00010110	22	7
10001110	00001101	13	.
10011011	00011000	24	9
10011110	00011101	29	>

Table 9: substitution method

Intermediate cipher text 1	Decimal equivalent	P=(n+value)% k0	plaintext(p)
8	23	82	s
*	9	68	e
(	7	66	c
:	25	84	u
7	22	81	r
.	13	72	i
9	24	83	t
>	29	88	y

At the end of decryption, original plaintext is**:** **security**

V. ADVANTAGES

1. Key generation is done by two techniques, one is raster scan and other is store and forward which enhances more security for the data.
2. Column wise retrieval process is one of the flavor added in this paper, which provides complexity to break the data.
3. Nibble swapping is another flavor, which enhance secure for the data.

VI. LIMITATIONS

It is applicable only for 94 characters.

VII. CONCLUSION

For protecting the information, the most popular approach is cryptography. The main aim of cryptography is the intended receiver can only understand the message. The proposed algorithm is providing better security than the existing algorithm. The existing algorithm uses arithmetic and logical operations, substitution method only. The proposed algorithm generates two keys from two different methods. Encryption algorithm consists substitution, column wise retrieving, and nibble swapping methods which are difficult to break. It is applicable for maximum length of the message. In the future work, this algorithm will be extended to use the UNICODE system support and row and column mixed retrieval method.

REFERENCES

[1] Govind Prasad Arya, Aayushi Nautiyal, ashish Pant, Shiv Singh & Tishi Handa, "*A cipher design with Automatic key generation using the combination of substitution and transposition techniques and basic arithmetic and logic operations*," the SIJ Transactions on computer science engineering & its applications (CSEA), Vol. 1, No. 1,March -April 2013.

[2] S.G.Srikantaswamy and Dr.H.D.phaneendra, " *A cipher design using the combined effect of arithmetic and logic operations with substitutions and transposition techniques* , " International Journal of Computer Applications (0975-8887),vol.29,no.8,pp.34-36.

[3] Ayushi, " A Symmetric Key Cryptographic Algorithm". International Journal of Computer Applications (0975 –8887), Volume.1, No.15.

[4] R.Venkateswaram, Dr.V.Sundaram, (2010) *Information Security: Text Encryption and Decryption with Poly Substitution method and combining features of cryptography*.

[5] Sania Jawaid, Adeeba Jamal," Generating the Best Fit Key in Cryptography using Genetic Algorithm", *International Journal of Computer Applications (0975 – 8887 Volume 98 – No.20, July 2014.*

[6] Sindhuja K and Pramela Devi S, "A Symmetric Key Encryption Technique Using Genetic Algorithm",Sindhuja Ketal, / (IJCSIT) International Journal of Computer Science and Information Technologies, ISSN:0975-9646 Vol. 5 (1), 2014, pg 414-416.

[7] Prof K.Govinda, Dr.E.Sathiyamoorth," multilevel cryptography technique using graceful codes", Journal of Global Research in Computer Science (jgrcs), Volume 2, sNo. 7, July 2011.

Authors Profile

Dr.S.Kiran is Assistant Professor in the department of Computer Science and Engineering at Yogivenama University , Proddatur. He acquired M.Tech Degree from Nagarjuna University, Guntur. He completed Ph.D in computer science from S.K.University. He has been continuously imparting his knowledge to several students in research activities. He published many articles National and International journals .. His research areas are image Processing, Cryptography and Network Security , Software Engineering and Data mining and Data ware house.

B. Reddaiah received his Ph.D Degree in Computer Science and Engineering in 2015 from Acharya Nagarjuna University, Andhra Pradesh. He is working as Assistant Professor in the Department of Computer Science and Engineering at YSR Engineering College of Yogi Vemana University, Proddatur. He has attended many workshops and published many papers in National and International Journals.

D Naga Sravanthi is a student in the department of Computer Science and Engineering at Y.S.R Engineering College of Y.V.U, Proddatur . She is studying 4th B.Tech in CSE. She attended many workshops , Seminars and published papers in national and International journals.

J Venkata Sivajaya Sree is a student in the department of Computer Science and Engineering at Y.S.R Engineering College of Y.V.U, Proddatur . She is studying 4th B.Tech in CSE. She attended many workshops ,Seminars and published papers in national and International journals.